CODEC NET

Security Operations Center

Quarterly Report

Codec Networks Pvt. Ltd.

Executive Summary

Report Period: July 27, 2025 - October 25, 2025

Top 10 Security Alerts

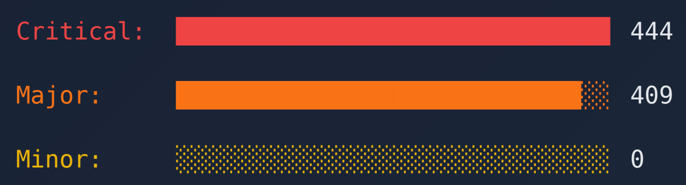
#	Severity	Alert Description	Host/Agent	Count	Last Seen
1	Major	syslog: User missed the password more than one time	wazuh-virtual-machine	147	08/06/25 12:05 PM
2	Major	Maximum authentication attempts exceeded.	wazuh-virtual-machine	135	08/06/25 12:05 PM
3	Critical	high-severity alert: custom malicious activity detected	wazuh-virtual-machine	122	09/09/25 5:51 PM
4	Critical	high-severity alert: Server resource utilization spiked unusually, possible DoS activity in progress.	wazuh-virtual-machine	117	10/14/25 12:48 PM
5	Critical	DNS request to C2 domain observed.	wazuh-virtual-machine	72	10/14/25 1:04 PM
6	Critical	igh-severity alert: custom malicious activity detected	wazuh-virtual-machine	60	08/08/25 12:15 PM
7	Critical	high-severity Brute-force login attempts detected.	wazuh-virtual-machine	57	10/14/25 12:56 PM
8	Major	Multiple authentication failures.	wazuh-virtual-machine	35	08/06/25 12:05 PM
9	Major	PAM: Multiple failed logins in a small period of time.	wazuh-virtual-machine	23	08/06/25 12:05 PM
10	Major	Windows application error event.	Windows_10_quarantine	17	09/10/25 4:20 PM

Alert Statistics & Trends

Alert Distribution

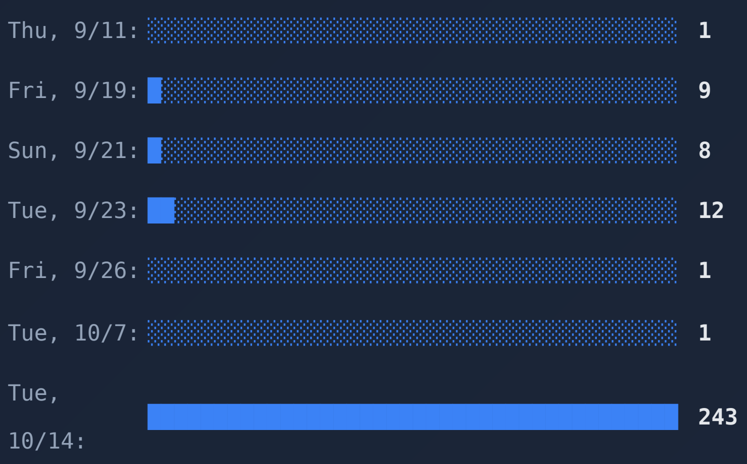
Critical	444
Major	409
Minor	0
Total Alerts	853

Alert Severity Breakdown



Critical: 52.1% | Major: 47.9% | Minor: 0%

Daily Alert Trend (Last 7 Days)



Top 5 Alert Types

syslog	330
High Alertscustom	248

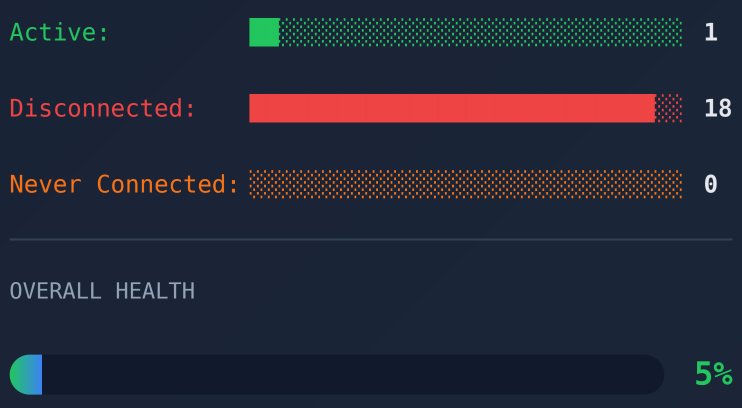
windows	30
pam	23

Agent Status Overview

Agent Summary

Total Agents	19
Active	1
Disconnected	18
Never Connected	0

Agent Health Status



Agent Details

wazuh-virtual-machine
Active

OS: Ubuntu
IP: 127.0.0.1
Version: Wazuh v4.12.0
Last Seen: 1/1/10000, 5:29:59 AM

Windows_10
Disconnected

OS: Microsoft Windows 10 Pro
IP: 192.168.1.30
Version: Wazuh v4.12.0
Last Seen: 7/7/2025, 3:24:41 PM

Kali_Docker
Disconnected

OS: Kali GNU/Linux
IP: 192.168.1.44
Version: Wazuh v4.12.0
Last Seen: 7/9/2025, 5:45:57 PM

BK_Kali
Disconnected

OS: Kali GNU/Linux
IP: 192.168.1.26
Version: Wazuh v4.12.0
Last Seen: 7/23/2025, 3:23:38 PM

Windows_10_old
Disconnected

OS: Microsoft Windows 10 Pro
IP: 192.168.1.15
Version: Wazuh v4.12.0
Last Seen: 7/14/2025, 4:58:34 PM

Windows_10_new
Disconnected

OS: Microsoft Windows 10 Pro
IP: 192.168.1.15
Version: Wazuh v4.12.0
Last Seen: 7/14/2025, 5:29:41 PM

OS: Kali GNU/Linux
IP: 192.168.174.128
Version: Wazuh v4.12.0
Last Seen: 8/30/2025, 2:26:00 PM

OS: Microsoft Windows 10 Pro
IP: 192.168.1.11
Version: Wazuh v4.12.0
Last Seen: 9/10/2025, 5:25:47 PM

CIS Compliance Status

Overall Compliance Score

36%

Security Configuration Assessment - Per Policy

CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 (773 passed, 1567 failed)	33%
CIS Microsoft Windows Server 2025 Benchmark (456 passed, 978 failed)	32%
CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0. (412 passed, 530 failed)	44%
CIS Distribution Independent Linux Benchmark v2.0.0. (256 passed, 294 failed)	47%
CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0. (100 passed, 145 failed)	41%

Agent Compliance Scores

1. BK_Kali
87 passed, 97 failed (1 policies)
47%

2. BK_Kali_new
87 passed, 97 failed (1 policies)
47%

45%

4. wazuh-virtual-machine
86 passed, 110 failed (1 policies)
44%

5. Linux_quarantine_2.0
87 passed, 109 failed (1 policies)
44%

6. Linux_quarantine_3.0
87 passed, 109 failed (1 policies)
44%

7. Yara_Ubuntu
76 passed, 101 failed (1 policies)
43%

8. Test_Linux_all
76 passed, 101 failed (1 policies)
43%

9. Linux_quarantine
100 passed, 145 failed (1 policies)
41%

10. mmad2
135 passed, 224 failed (1 policies)
38%

11. mmad1
129 passed, 230 failed (1 policies)
36%

12. Windows_10_old
130 passed, 260 failed (1 policies)
33%

13. test_windows_all
128 passed, 262 failed (1 policies)
33%

14. test_windows
128 passed, 262 failed (1 policies)
33%

130 passed, 260 failed (1 policies)

16. Windows_10_quarantine
127 passed, 263 failed (1 policies)
33%

17. Windows_10
130 passed, 260 failed (1 policies)
33%

18. mmadpay2
96 passed, 262 failed (1 policies)
27%

19. mmadpay1
96 passed, 262 failed (1 policies)
27%

Configuration Findings Summary

Total Checks	5511
Passed	1997
Failed	3514

Executive Summary

Overview

During the reporting period of July 27, 2025 - October 25, 2025, our Security Operations Center monitored and analyzed 853 security alerts across your infrastructure. The alert distribution shows 444 critical alerts, 409 major alerts, and 0 minor alerts.

Our team has been actively monitoring, triaging, and responding to security events in real-time. 19 agents are deployed across your infrastructure, with 1 currently active.

Security configuration assessment shows an overall compliance score of 36% with 3514 failed checks requiring attention.